4. Варченко І. Реформи в Грузії 2004-2012 років: уроки для України. URL: http://blogs.lb.ua/ivan_varchenko/283375_reformi_gruzii_rokiv.html.

5. Предотвращение коррупции на отраслевом уровне в странах Восточной Европы и Центральной Азии (на примере сферы образования, добывающей отрасли и полиции). URL: https://www.oecd.org/corruption/acn/OECD-ACN-Study-Corruption-Prevention-Sector-Level-2017.

6. Безкарність та недієве правосуддя тримають Україну на корупційному дні. URL: https://ti-ukraine.org/research/indeks-koruptsiyi-cpi-2016.

7. Про запобігання корупції: Закон України від 14.10.2014 № 1700-VII // Відомості Верховної Ради України. 2014. № 49. Ст. 2056.

Вишня Володимир Борисович
д.т.н., проф., професор кафедри
Гавриш Олег Степанович
викладач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ;

ІНФОРМАЦІЇНА ВІЙНА НА СУЧАСНОМУ ЕТАПІ РОЗВИТКУ СУСПІЛЬСТВА

Сьогодні інформатизація суспільства веде нас до створення єдиного світового інформаційного простору, в рамках якого проводиться накопичення, обробка, зберігання та обмін інформацією між суб'єктами цього простору – населенням, організаціями, державами.

Очевидно, що можливості швидкого, політичною, економічною, науково-технічної та іншою інформацією, застосування нових технологій у всіх сферах суспільного життя і особливо у виробництві і управлінні є безсумнівним благом. Однак, швидкий розвиток промисловості стало загрожувати екології планети, а досягнення в галузі ядерної фізики породили небезпеку ядерної війни. Інформація теж може стати джерелом серйозних проблем.

Всім давно відомо широко поширене, дуже лаконічне, і в той же час ємне визначення поняття «війна», яке даввидатний військовий теоретик фон Клаузевіц, зокрема,«війна – це продовження політики іншими засобами, коли перо дипломата змінюється на багнет військового». Так було протягом всієї історії людства.Цілі цивілізації виникли, виросли, постаріли і загинули на війні. Згодом ведення війни перетворилося на цілу науку. Технічний прогрес завжди був самим вірним супутником війни.

Сучасна військова думка зробила крок далеко вперед. Тепер її сфера – усяпланета. У військових доктринах різних країн світу все частіше виявляються згадки про програми розвитку електронного зброї і програмного забезпечення спеціального призначення. Інформаційна війна розглядається як можливість стратегічної альтернативи в тих країнах, де розуміють, що при веденні бойових дій звичайними засобами вони явно поступаються.

Сам термін «інформаційна війна» зобов'язаний своїм походженням військовим і з'явився в середині 1980-х років в зв'язку з новими завданнями Збройних сил США після закінчення «холодної війни». Термін почав активно вживатися

після проведення операції «Буря в пустелі» в 1991 році, коли нові інформаційні технології вперше були використані як засоби ведення війни. Термін офіційно закріплений в директиві Міністерства оборони США від 21 грудня 1992 року. У військових колах США під інформаційною війною розуміються дії, що вживаються для досягнення інформаційної переваги в підтримці національної військової стратегії за допомогою впливу на інформацію та інформаційні системи супротивника, при одночасному забезпеченні безпеки і захисту власної інформації та інформаційних систем.[1]

До особливостей інформаційної війни можна віднести наступне:

- інформаційна війна охоплює в якості самостійних об'єктів всі види інформації та інформаційних систем, відокремлюючи інформацію від середовища використання;

- об'єкти можуть виступати як зброя, так і об'єкт захисту;

- інформаційна війна розширює територію і простір ведення військових дій, ведеться як при оголошенні війни, так і в кризових ситуаціях;

- інформаційна війна ведеться як спеціалізованими військовими, так і цивільними структурами.

Інформаційна війна включає дії, що вживаються для досягнення переваги в забезпеченні національної військової стратегії шляхом впливу на інформаційні системи противника і одночасне зміцнення і захист власних.

Інформаційна війна являє собою всеосяжну цілісну стратегію, покликану віддати належне значущості і цінності інформації в питаннях командування, управління і виконання наказів збройними силами і реалізації національної політики. Така війна націлена на всі можливості і чинники уразливості, що неминуче виникають при зростанні залежності від володіння інформацією, а також на використання інформації у всіляких конфліктах.

Об'єктом уваги стають інформаційні системи (включаючи лінії передач, обробні центри та людські фактори цих систем), а також інформаційні технології, що використовуються в системах озброєнь. Великомасштабне протистояння між громадськими групами або державами має на меті змінити розстановку сил в суспільстві.

Інформаційна війна включає наступальні і оборонні складові.

Інформаційна зброя може використовуватися з «електронними швидкостями» при нападі й обороні. Вона базується на самих передових технологіях і покликана забезпечити вирішення військових конфліктів на ранній стадії, а також виключити застосування сил загального призначення. Стратегія застосування інформаційної зброї носить наступальний характер. Однак є розуміння власної вразливості, особливо громадянського сектора, тому проблеми захисту від такої зброї та інформаційного тероризму сьогодні виходять на перший план. Останню обставину необхідно пам'ятати керівництву багатьох державних і корпоративних мереж, які активно працюють в Інтернеті і мають намір підключатися до інших глобальних телекомунікаційних мереж. Уразливість національних інформаційних ресурсів країн, що забезпечують своїм користувачам роботу в світових мережах, – річ двосічна. Інформаційні ресурси противників взаємно уразливі.

Теоретики нерідко відносять до цього виду зброї різні способи інформаційного впливу на противника: від дезінформації і пропаганди до радіоелект-

ронної боротьби. Однак інформаційною зброєю точніше було б назвати засоби знищення, перекручення або розкрадання інформаційних масивів, засоби подолання систем захисту, обмеження допуску законних користувачів, дезорганізації роботи апаратури і комп'ютерних систем в цілому.

Атакуючою інформаційною зброєю сьогодні можна назвати:

- комп'ютерні віруси, здатні розмножуватися, впроваджуватися в програми, передаватися по лініях зв'язку і мереж передачі даних, виводити з ладу системи управліннят.ін.;

- логічні бомби – запрограмовані пристрої, які впроваджують в інформаційно-керуючі центри військової або цивільної інфраструктури, щоб по сигналу або у встановлений час привести їх в дію;

- засоби придушення інформаційного обміну в телекомунікаційних мережах, фальсифікація інформації в каналах державного та військового управління;

- помилки різного роду, що свідомо вводяться в програмне забезпечення об'єкта.

Універсальність, скритність, відмінність способів програмно-апаратної реалізації, радикальність впливу, можливість вибору часу і місця застосування, нарешті, економічність роблять інформаційну зброю надзвичайно небезпечною: її легко замаскувати під засоби захисту, скажімо, інтелектуальної власності; крім того, вони дозволяють навіть вести наступальні дії анонімно без оголошення війни.

Оборонно-розвідувальне агентство США опублікувало звіт про розслідування джерел кібератак на національні сайти. Результати здивували американських військових: 80% хакерськихздійснюється з території Канади. Директор ФБР назвав Канаду притулком хакерів.

Інформаційні пірати, сліди яких ведуть до Швеції, вкрали програму супутникової навігації американського флоту. Цікаво, що хакери використовували при цьому комп'ютерну мережу німецького університету, працюючи під час різдвяних канікул. Хакери завдали при цьому збитків на величезну суму. Одна лише ліцензія на використання навігаційної програми протягом року коштує 60 млн доларів.

Один з китайських генералів висловив таку думку: «Ми цілком могли б паралізувати командний пункт супротивника, який при отриманні дезінформації буде приймати неправильні рішення. У нас є можливість встановити контроль над банківською системою противника і над суспільством в цілому ».

У пресі повідомлялося, що витончені спроби зламати комп'ютери Пентагону, до яких вдавався протягом трьох років, ймовірно, були здійснені з відома російської влади російськими хакерами.

Цікаво, що як Китай, так і Росія проявляють інтерес до будь-яких форм співпраці з іншими державами, які могло б перешкодити подібним атакам.

Проблема інформаційного вторгнення в комп'ютерні мережі з застосуванням інформаційної зброї зараз актуальна як ніколи. Вихід цієї загрози на перший план пов'язаний з тим, що сучасні системи управління є системами з високим рівнем комп'ютеризації. Вони можуть виявитися вельми уразливими з точки зору впливу інформаційної зброї в мирний і воєнний час. Такий вплив може привести до того, що у загрозливий період зброю стримування країни, що зазнала агресії, за рахунок прихованого впровадження закладок в програмне забезпечення систем управління виявиться повністю або частково заблоко-

ваним. Про реальність цього твердження свідчить досвід війни в Перській затоці. Ірак практично не зміг застосувати закуплені у Франції системи ППО, тому що їх програмне забезпечення містило логічні бомби, які були активізовані з початком бойових дій.

Американські військові вважають, що перевага в інформаційному зброї повинно зміцнити світове лідерство США. Цим пояснюється великий інтерес і активність американців в дослідженні проблем інформаційної війни. Все сказане підтверджується доповідями і дискусіями на міжнародних конференціях по інформаційній війні, більшість учасників яких складають співробітники державних установі, армії і розвідувальнихцентрів США.

Ось уже кілька років провідні вищі навчальні заклади армії США, зокрема Національний університет оборони у Вашингтоні і Військово-морський коледж в Ньюпорті, випускають таких військових професіоналів, як фахівці з інформаційної війни. Інше, не менш могутнє відомство – ЦРУ – вже кілька років виконує надсекретну програму по впровадженню в усі чіпи, вироблені американськими компаніями для потужних комп'ютерних систем, як на території США, так і за її межами, логічних бомб, які при отриманні особливого сигналу (наприклад , з супутника) можуть викликати збої в роботі цих систем або зовсім вивести їх з ладу. При цьому немає відкритих даних про новітні методи ведення військових дій і, взагалі, про принципово нову зброю – інформаційному. Відсутні повні дані і про масштаби інформаційного тероризму, який в останні два-три роки придбав вже глобальний характер. Є дані про те, що деякі терористичні організації отримали можливість використовувати в своїх цілях навіть супутникові транспондери – канали, через які можна маніпулювати інформацією.

У сучасному суспільстві військова стратегія використання інформаційної зброї виявилася тісно пов'язаною з громадянським сектором і стала багато в чому від нього залежати. Різноманітність інформаційної зброї, форм і способів її впливу, особливості появи і застосування породили складні завдання захисту від неї.Вважається, що для запобігання або нейтралізації наслідків застосування інформаційної зброї необхідно вжити такі заходи:

- захист матеріально-технічних об'єктів, що становлять фізичну основу інформаційних ресурсів;
- забезпечення нормального і безперебійного функціонування баз і банків даних;
- захист інформації від несанкціонованого доступу, її перекручення чи знищення;
- збереження якості інформації (своєчасності, точності, повноти і необхідної доступності).

Створення технологій виявлення впливів на інформацію, в тому числі у відкритих мережах, – це природна захисна реакція на появу нової зброї. Економічну і науково-технічну політику підключення держави до світових відкритих мереж слід розглядати через призму інформаційної безпеки. Будучи відкритою, орієнтованої на дотримання законних прав громадян на інформацію та інтелектуальну власність, ця політика повинна передбачати захист мережевого обладнання на території країни від проникнення в нього елементів інформаційної зброї. Це особливо важливо сьогодні, коли здійснюються масові закупівлі зарубіжних інформаційних технологій.

Зрозуміло, що без підключення до світового інформаційного простору країну очікує економічнийзанепад. Оперативний доступ до інформаційних і обчислювальних ресурсів, зрозуміло, слід вітати як фактор подолання міжнародної ізоляції і внутрішньої дезінтеграції, як умову зміцнення державності, інститутів громадянського суспільства, розвитку соціальної інфраструктури.

Однак слід чітко уявляти, що участь країни в міжнародних системах телекомунікацій та інформаційного обміну неможливо без комплексного вирішення проблем інформаційної безпеки. Особливо гостро проблеми захисту власних інформаційних ресурсів у відкритих мережах постають перед країнами, які технологічно відстають від США або Західної Європи в області інформаційних і телекомунікаційних технологій. До числа таких країн, на жаль, відноситься і Україна. Сьогоднішній стан нашої економіки, нерозвиненість інформаційної інфраструктури, непідготовленість українських користувачів до ефективної роботи у відкритих мережах, не дозволяють реалізувати повноцінну участь країни в таких мережах і користуватися всіма новими технологіями.

Заборонити розробку і застосування інформаційної зброї, як це зроблено, наприклад, для хімічної чи бактеріологічної зброї, навряд чи можливо. Так само неможливо обмежити зусилля багатьох країн щодо формування єдиного глобального інформаційного простору.

Слід пам'ятати про захист національних інформаційних ресурсів та збереженні конфіденційності інформаційного обміну по світових відкритих мережах. Цілком ймовірно, що на цьому підгрунті можуть виникати політичні та економічні конфронтації держав, нові кризи в міжнародних відносинах. Тому інформаційна безпека, інформаційна війна і інформаційна зброя виявилися в центрі уваги.

---

1. Інформаційні війни в політичному житті на прикладі мас-медіа Росії та США [Електронний ресурс]. – Режим доступу: http://ua-reference.com/Інформаційні_війни_в_політичному_житті_на_прикладі_мас-медіа_Росії_та_США.

Денисов Сергій Федорович
д.ю.н., проф., завідувач кафедри
кримінального, кримінально-виконавчого
права та кримінології

Пузиревський Максим Вячеславович
начальник кабінету кафедри
тактико-спеціальної підготовки
Академії Державної пенітенціарної служби

КРИМІНОЛОГІЧНИЙ ПОРТРЕТ ОСОБИ ЗЛОЧИНЦЯ: ПОНЯТТЯ, ЗМІСТ І ЗНАЧЕННЯ ДЛЯ ЗАПОБІГАННЯ ЗЛОЧИННИМ ПРОЯВАМ

Проблема особи злочинця є однією з основних і водночас найбільш складних проблем в доктрині сучасної кримінології. Посідаючи провідне місце в ланцюгу кримінологічної причинності, особа злочинця є основним об’єктом профілактичного впливу з метою запобігання вчиненню злочинів. Саме тому,